THE SPECIFICATION

Please replace the paragraph beginning on page 5, line 21 and ending on page 6, line 8 with the following revised paragraph:

B1

Another secure boot model, known as AEGIS®, is disclosed by W. Arbaugh, D.G. Farber, and J.M Smith in a paper entitled "A Secure and Reliable Bootstrap Architecture", Univ. of Penn. Dept. of CIS Technical Report, IEEE Symposium on Security and Privacy, page 65, 1997. This AEGIS® model requires a tamper-resistant BIOS that has hard-wired into it the signature of the following stage. This scheme has the very considerable advantage that it works well with current microprocessors and the current PC architecture, but has three drawbacks. First, the set of trusted operating systems or trusted publishers must be wired into the BIOS. Second, if the content is valuable enough (for instance, e-cash or Hollywood videos), users will find a way of replacing the BIOS with one that permits an insecure boot. Third, when obtaining data from a network server, the client has no way of proving to the remote server that it is indeed running a trusted system.

Please replace the paragraph on page 6, lines 9-14 with the following revised paragraph:

B1

On the more general subject of client-side rights management, several systems exist or have been proposed to encapsulate data and rights in a tamper-resistant software package. An early example is IBM®'s Cryptolope®. Another existent commercial implementation of a rights management system has been developed by Intertrust. In the audio domain, AT&T® Research have proposed their "A2b®" audio rights management system based on the PolicyMaker rights management system.